MULTICOMMMANAGER
USER GUIDE

MultiTech®
Systems

MultiCommManager User Guide

P/N 82011208, Revision I

Copyright © 1997 by Multi-Tech Systems, Inc.

Revision	Date	Description
H	9/15/97	Documents MultiModemManager version 6.12.
I	11/21/97	Documents MultiCommManager version 7.00.

Software User License Agreement

MultiCommManager software is licensed by Multi-Tech Systems, Inc. to the original end-user purchaser of the product, hereafter referred to as "Licensee." The License includes the distribution diskette, other accompanying programs, and the documentation. The MultiCommManager software, hereafter referred to as "Software," consists of the computer program files included on the original distribution diskette.

Licensee agrees that by purchase and/or use of the Software, he hereby accepts and agrees to the terms of this License Agreement.

In consideration of mutual covenants contained herein, and other good and valuable considerations, the receipt and sufficiency of which is acknowledged, Multi-Tech Systems, Inc. does hereby grant to the Licensee a non-transferable and non-exclusive license to use the Software and accompanying documentation on the following conditions and terms: The software is furnished to the Licensee for execution and use on a single computer system only and may be copied (with the inclusion of the Multi-Tech Systems, Inc. copyright notice) only for use on that computer system. The Licensee hereby agrees not to provide or otherwise make available any portion of this software in any form to any third party without the prior express written approval of Multi-Tech Systems, Inc.

Licensee is hereby informed that this Software contains confidential proprietary and valuable trade secrets developed by or licensed to Multi-Tech Systems, Inc. and agrees that sole ownership shall remain with Multi-Tech Systems, Inc.

The Software is copyrighted. Except as provided herein, the Software and documentation supplied under this agreement may not be copied, reproduced, published, licensed, sub-licensed, distributed, transferred, or made available in any form, in whole or in part, to others, without expressed written permission of Multi-Tech Systems, Inc. Copies of the Software may be made to replace worn or deteriorated copies for archival or backup procedures.

Licensee agrees to implement sufficient security measures to protect Multi-Tech Systems, Inc. proprietary interests and not to allow the use, copying or transfer by any means, other than in accordance with this agreement. Licensee agrees that any breach of this agreement will be damaging to Multi-Tech Systems, Inc.

Licensee agrees that all warranties, implied or otherwise, with regard to this Software, including all warranties of merchantability and fitness for any particular purpose are expressly waived, and no liability shall extend to any damages, including consequential damages, whether known to Multi-Tech Systems, Inc. It is hereby expressly agreed that Licensee's remedy is limited to replacement or refund of the license fee, at the option of Multi-Tech Systems, Inc., for defective distribution media. There is no warranty for misused materials.

This package contains 3.5-inch disks. Neither this software nor the accompanying documentation may be modified or translated without the written permission of Multi-Tech Systems, Inc.

This agreement shall be governed by the laws of the State of Minnesota. The terms and conditions of this agreement shall prevail regardless of the terms of any other submitted by the Licensee. This agreement supersedes any proposal or prior agreement. Licensee further agrees that this License Agreement is the complete and exclusive statement of Agreement, oral, written, or any other communications between Multi-Tech Systems, Inc. and Licensee relating to the subject matter of this agreement. This agreement is not assignable without written permission of an authorized agent of Multi-Tech Systems, Inc.

Contents

1 Introduction

2 Installation

3 Getting Started

4 Organizing and Configuring Your Modems

5 Security

6 Monitoring and Controlling Your System

7   Solving Problems

8   Warranty, Service, and Technical Support

Index

1 Introduction

Introduction

MultiCommManager, model MMMSNMP, is a major update of Multi-Tech's MultiModemManager rack and modem management software. MultiCommManager is a software suite that centralizes control and configuration of rack controllers, rack-mounted analog and digital communication devices, stand-alone or unmanaged rack-mounted modems, and RASExpress communication servers. The system administrator can use it to change rack and device configurations, analyze performance, control access to devices for security, and monitor all connections.

Description

MultiCommManager consists of four modules: the Manager, the Configuration Manager, the Statistical Analyzer, and the Security Database Editor:

- The *Manager* provides organization of modems through logical groupings; visual feedback on system status; control over callback security options, fault and alarm status, and corrective actions; diagnostic tools for testing, verifying, and tracking modem operation; and automated modem configuration.

  The Manager tracks connections and faults in near-real time, giving you up-to-the-moment troubleshooting and reporting information that allows you to respond to minor problems before they cause major breakdowns.

  The Manager can configure and monitor all devices in a CommPlete rack, including T1 interfaces, modems, and power supplies, and PRI cards when they become available.

  A new feature of the Manager is that it can also configure remote access servers running Multi-Tech RASExpress software, and can display RASExpress server setup information, statistics, and user IDs. Thus, it no longer necessary to run the RASExpress Remote Utilities for Windows to configure your servers.

- The *Statistical Analyzer* performs statistical analyses of event data and generates connection reports, log reports, and graphs of the analyzed data. The Statistical Analyzer can analyze and report data from one of your sites or all. Reports can include information on communication device connections, system faults, and utilization. Reports can be generated in ASCII, dBASEIII™, and ASCII delimited formats. Reports for RASes and T1 lines will be added in the near future.

- The *Configuration Manager* exists for MultiModemManager legacy support. It enables the administrator to create custom configuration files for modems. Each modem is associated with

a configuration file stored in flash memory in the MR4800E rack controller or on the hard disk of an independent management PC. Because configuration files can be assigned to one or more modems, the configuration of a group of modems can be changed by editing a single file.

- The *Security Database Editor* also exists for MultiModemManager legacy support. It enables the administrator to create and maintain a security database of system users for MR4800 and MR4800E racks. A database record includes the user ID, password, valid dates and times of access, and security type.

For detailed information about how to use the menus, commands, and dialog boxes in these modules, please see MultiCommManager Help.

Local Sites vs. Remote Sites

MultiCommManager can manage both local sites and remote sites. What is the difference?

- A *local site* is one or more racks connected to the management console through an Arcnet card called the Management Interface Card, or MIC. Local sites are also known as MultiModemManager legacy link sites, because they typically consist of MultiModemManager racks with MR4800 controllers. Thus, "local," "legacy," and "MultiModemManager legacy link" all refer to the same thing.

  If the Manager is configured as an agent, it can act as an SNMP proxy agent for the local racks and can be managed by a third party SNMP manager or by a Manager configured as a supervisor.

- A *remote site* is an SNMP rack that can be managed through the Internet. It need not be physically remote from the management console. Remote sites can be MultiModemManager racks with MR4800E controllers or CommPlete Communications Server racks with MR9600 controllers.

Typographic Conventions

Certain typographic conventions have been adopted throughout the text of this manual to illustrate keyboard input, screen display dialogs, and special vocabulary.

- Text entered by you is shown in bold. Example: **supervisor**.

- Dialog box titles, menu titles, commands, and options are also shown in bold. Example: **Help** menu.

- Menu paths are abbreviated by the use of vertical bars. For example, "Select **Setup | Modem | Security | Messages**" means to click the **Setup** menu in the menu bar, click **Modem**, click **Security**, and finally click **Messages**.

- Screen messages are shown in a `monospace` font.

- Italics are used for important new terms, for book and manual titles, and when terminology is explained, introduced, or emphasized. Example: "The word *bit* is a contraction of the words *binary digit.*").

- Names of keyboard keys are shown in small caps. Example: SHIFT.

- Certain keys and key combinations may be abbreviated as follows:

  <CR>   Means press the carriage return key, which can be represented on the keyboard by a broken left-pointing arrow or the words *Enter* or *Return*. The ENTER key, or carriage return, is often used to activate commands.

  ALT+X   Means to hold down the ALT key while you press the key represented by X.

  CTRL+X   Means to hold down the CTRL (control) key while you press the key represented by X.

- Please notice the difference between the capital letter *O* and the number *0.*

2   Installation

Introduction

This chapter describes how to install MultiCommManager on a management workstation. The workstation should have access to your LAN and/or the Internet, or be connected to your MultiModemManager rack by a Management Interface Card (MIC). The minimum requirements for the workstation are a 486DX/33 microprocessor, 8 MB of RAM, 50–100 MB of hard disk space, a 3.5-inch floppy drive, an Ethernet network interface card (NIC) or Arcnet card (MIC), a VGA monitor, a two-button mouse, and Windows 3.11, Windows 95, or Windows NT 3.1 or higher.

MultiCommManager is provided on two 3.5″diskettes.

How to Install MultiCommManager

1. Turn on the workstation and start Windows.

2. Make working copies of your MultiCommManager diskettes, label the copies, and store the original diskettes in a safe place.

3. Insert disk 1 into the workstation's floppy drive.

4. To run the Setup program, find A:\SETUP.EXE using File Manager or Windows Explorer, and double-click it.

   Follow the instructions in the Setup program. By default, Setup copies the MultiCommManager files to the directory C:\MRACK. Do not install MultiCommManager over an existing version of the MultiModemManager software. Install it to a different directory instead. A new program group, called MultiCommManager, is added to the Program Manager or the Start menu.

5. The MultiCommManager program group contains icons for the Manager; the Configuration Manager; the Security Database Editor; the Statistical Analyzer; and several Read Me files.

6. To start MultiCommManager, double-click on the Manager icon.

3   Getting Started

Introduction

This chapter is a brief guide to setting up MultiCommManager for use with your racks and modems. For more detailed information see the online Help.

The Manager

To start MultiCommManager, double-click the Manager icon. The Manager module's main window appears.
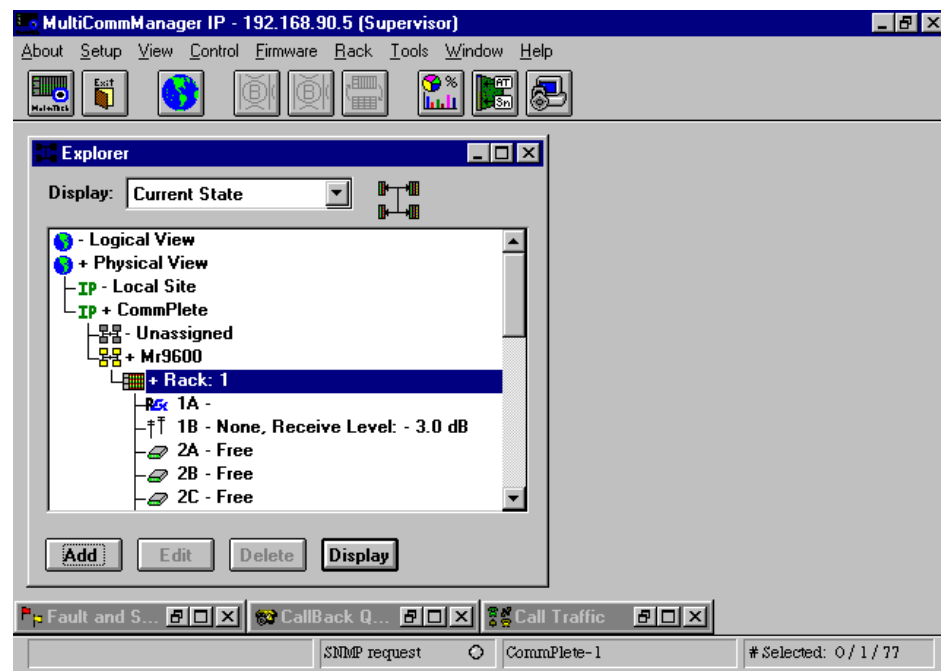
The Manager module enables you to organize, monitor, and control your communications devices through a graphic user interface called the *Explorer*. Using the Explorer, you can select the modems that you want to review, hang up, reset, put out of service, or configure.

The Fault and Status Events window, the Call Traffic window, and the Call Back Queue window give run-time analyses of system functions. These windows are always available in the client area of the main window, whether expanded or minimized.

The Manager can monitor faults and respond to them when a previously set threshold has been reached. Using the Pager function, the Manager can notify a system administrator of problems through a digital or text pager. It also can log system events for later analysis of system performance by the Statistical Analyzer.

The Manager also can configure remote access servers running Multi-Tech RASExpress software, and can display RASExpress server setup information and statistics. Thus, it no longer necessary to run the RASExpress Remote Utilities for Windows to configure your servers.

Note: The Callback Queue window and the local Call Traffic window (the one that is always present) are not used with CommPlete racks. You can open a Call Traffic window for a CommPlete rack by selecting its IP site and clicking **Display**.

The Explorer

The Explorer is your window on the operation of your communications system. Use it to display, organize, and configure your communications racks and devices. Explorer is organized in an inverted tree structure. You can expand or collapse your view of the structure by double-clicking any icon but the T1, phone line, or device icon. At the root are two views of your system: a physical view and a logical view.

To open the Explorer, click the Explorer button on the toolbar. When you first run the Manager, the Explorer window is open by default. (The Manager saves the current desktop when you exit.)

The Physical View

The physical view maps the physical organization of your communication devices. Devices are organized by racks, racks by rack groups, and rack groups by IP sites. An IP site is defined by its IP address. A rack group is an arbitrary grouping of racks at an IP site. When a rack has its own IP address, as in a CommPlete Communications Server, there is only one rack in the rack group.

The physical view also shows the TI lines and RASExpress servers for each rack. By double-clicking the RASExpress server icon, you can view the settings for its ISI (intelligent serial interface) circuits. By double-clicking an ISI icon, you can see the status of each serial port served by the ISI circuit.

The Logical View

The logical view maps the logical organization of your modems. The same modems are displayed as in the physical view; however, in the logical view you can assign them to modem groups. A modem group is an arbitrary grouping of modems at an IP site. You can group modems by how they are configured, by the hosts they connect to, by security type, by type of modem card, or by any other criteria that are useful to you. A modem or a rack of modems can be assigned to any modem group at the IP site at which it is located, but not to a modem group at another IP site. When an individual modem is assigned to a modem group, the rack in which the modem is installed appears as an identifier; therefore, the same rack can appear in several different modem groups.

The Local Site

Although it uses an "IP" icon, by definition the local site consists of one or more MultiModemManager racks connected to the management console by a local Arcnet link. Thus, the local site has no IP address or SNMP management. Regardless, all general references to IP sites in this manual and online Help should be understood to include the local site as well as remote sites, which do have IP addresses.

You can choose not to display the local site. To display the local site, select **Setup|Legacy Management|Show Local Site** and make sure the command has a check mark by it.

You might also have to configure MultiCommManager to talk to the management console's management interface card (MIC). To do this, select **Setup| Legacy Management|Management Interface Card** and make sure that the card is enabled and that the settings correspond to the switch settings on the card.

Unassigned Groups

Each site has a default **Unassigned** group, in which racks and modems are placed until the administrator can move them to a defined group. A defined group is a group that has been created by the system administrator. However, in the physical view the rack and modems at remote IP sites are automatically placed in a predefined group, so the **Unassigned** group is empty. In the logical view, racks and modems can be moved between modem groups by dragging.

Displaying Objects

The first time you start the Manager, the only objects displayed are the icons for the physical and logical views. To open an object, double click it. A closed object has a "-" in front of the object name; an open object has a "+". Remote IP sites are not displayed in the Explorer until they have been

defined by the administrator. To define an IP site, select a world icon, click the **Add** button, and enter the requested information in the **Add IP Site** dialog box.

To display a group at a site, double-click the site name. The group should appear with a yellow icon, indicating that there are active racks in the group. If the group icon is gray, then MultiCommManager is having trouble communicating with the racks attached to the group. For help on troubleshooting this kind of problem, see "Solving Problems" in the online Help.

If the group is yellow, double-click it to display the active racks under it, then double-click the racks to display the modems that are installed in them. From this point you can display rack and modem information in several different ways.

To display	Click
A graphic view of the rack	A rack icon, then the **Display** button
A graphic view of the modem	A modem icon, then the **Display** button
A modem's configuration file	The **Display** box, then **Configuration File**
A modem's basic setup	The **Display** box, then **General Setup**

Displaying Modems at Remote IP Sites

With MultiCommManager, you can display information about modems at remote sites, even halfway around the world. MultiCommManager can act as an SNMP proxy agent for racks and modems that are attached to it (it speaks SNMP for racks and modems that can't on their own). A MultiCommManager system that is running as an SNMP proxy is called an agent.

This section describes how a supervisor MultiCommManager can view modems that are attached to agents on the same TCP/IP network.

Running MultiCommManager as a Supervisor

To run MultiCommManager as a supervisor, you must be able to ping an agent's IP address. If you are unable to ping the agent, see "Solving Problems" in the online Help. When you can successfully ping the agent, run MultiCommManager. The title bar shows your IP address and the mode you are running in. The default mode is supervisor. To change to supervisor mode from another mode, select **Setup|SNMP| Mode|Supervisor**. The title bar changes to reflect your selection.

Displaying an Agent and Its Modems

To display information about an agent, add it to the list of IP sites that MultiCommManager monitors. To add an IP site, see "How to Add an IP Site" on the next page.

The IP icon of the new agent should be green. If it is not, see "Solving Problems" in the online Help. To view the agent's groups, double-click the icon for the IP site. You can now perform the same actions on these remote modems as on local modems.

Procedures for Setting Up Remote IP Sites

How to Set Up an Agent IP Site

1. Run MultiCommManager and select **Setup|SNMP|Mode|Agent**.

2. Select **Setup|SNMP|Default Trap IP**. In the **Set Default Trap IP** dialog box, type the IP address of the MultiCommManager supervisor that will be monitoring the agent site.

How to Add an IP Site

1. In the Explorer, select a world icon, then click Add.

2. In the Add IP Site dialog box, type the IP address of the MultiCommManager agent that you wish to display, and the long and short names for the site. The long name is used in the titles of windows that display information about objects from the site. The short name is used in the Fault and Status Events window to identify the IP site where a fault or status occurred.

3. Type the Get Community and **Set Community** settings to match the Get and Set Community settings of the agent that you are adding. (These are used for security purposes.) The default is **public**.

4. When you are finished, click **OK**. An IP site with the long name displayed should appear in the Explorer.

How to Edit an IP Site

1. To edit the settings for an IP site, find the IP site in the Explorer.

2. Click the IP site and then click **Edit.** You can change any of the settings for the site except the IP address.

3. To change a site's IP address, delete the old site and then add a new site with the new IP address and otherwise identical information.

How to Delete an IP Site

1. To delete an IP site, find the IP site in the Explorer.

2. Click the IP site and then click **Delete**. This will close all windows and open hierarchies in the Explorer that are related to the site.

The Statistical Analyzer

The Statistical Analyzer is a utility that analyzes and displays as graphs or reports events collected by MultiCommManager and controller logs. You can analyze the event data in several different ways, depending on the type of report desired. You can display the analyzed event data as pie charts or bar graphs. You can create connection reports and log reports in ASCII or dBASEIII format for import to a database. You can view a report in a text editor or send its contents to any Windows printer. Using the scrollable, read-only, Statistical Analyzer text viewer, you can display, print, or search any report.

To run the Statistical Analyzer from Windows, double-click on the Statistical Analyzer icon in the MultiCommManager program group or Start menu. To run it from the Manager, click the **Statistical Analyzer** button on the toolbar.
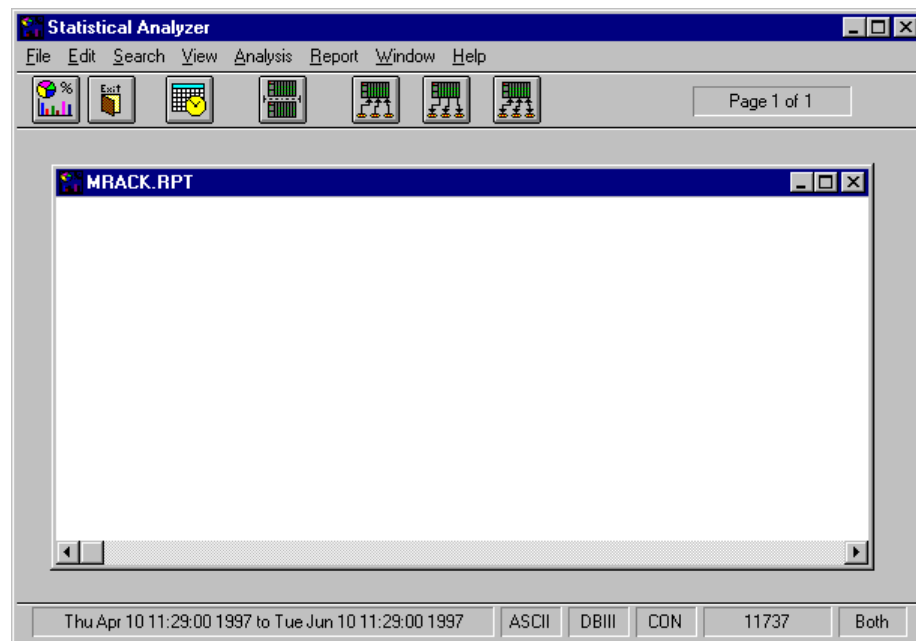
The Analysis Period

Your first step in analyzing data is to pick an *analysis period*. The analysis period is the time span for which you want to analyze the data. Graphic display of the analysis results is selected by default. The initial analysis can be refined by using call direction (inbound, outbound, or both) and modem filtering to select which modems should be used in the analysis.

The Analysis Data

The Statistical Analyzer looks for data in the C:\MRACK\MR.LOG\ directory of the management workstation. Data for the local site is stored as .EVT log files. Data for each remote site is stored in the remote controller as .HR log files. To analyze remote data, you must FTP the .HR files to a subdirectory of MR.LOG that has the same name as the short name of the remote site. E.g., for a remote site with the long name "CommPlete" and the short name "CMP," the .HR files must be placed in C:\MRACK\MR.LOG\CMP\. The subdirectory for each site is created automatically when you define the site.

Analysis Procedures

Analyzing data is a four-step process:

1. Decide on the IP site and period you want to analyze.

2. FTP log files for the period from the IP site to the management PC (not required for a local site).

3. Select analysis parameters in the **Analysis Period** dialog box and process the data.

4. Display the results.

The following procedures describe these steps in greater detail.

How to FTP Log Files to the Management Workstation

Note: This procedure is not required for a local site.

1. From the management workstation, use a third-party FTP utility to access the controller of the remote IP site that you want to analyze.

2. Change to the controller's B:\MMM\MR.LOG directory.

3. Select the .HR log files for the period that you want to analyze. The file names consist of four two-digit numbers that indicate the month, day, hour, and year that the log was open.

4. FTP the files to C:\MRACK\MR.LOG*xxx*\ in the management workstation, where *xxx* represents the short name of the remote IP site.

5. Exit the FTP utility.

How to Analyze Data

1. For a remote IP site, FTP the log files for the period you want to analyze to C:\MRACK\MR.LOG*xxx*\ in the management workstation, where *xxx* represents the short name of the remote IP site. For a local site, this step is not necessary.

2. Open the Statistical Analyzer.

3. Select **Analysis|Analysis Process**. The **Analysis Period** dialog box opens.

4. Select the IP site you want to analyze.

5. Select the start date and time and end date and time for the analysis period.

6. Select your output options.

7. Click **Process**. The data is analyzed.

How to Display the Results of an Analysis

1. Click the **View** menu.

2. Select your graph options (optional).

3. Click the parameter type you would like to view (**Connect Speed**, **Disconnections**, **Faults**, **Modem Usage**, etc.).

4. The results of the analysis are displayed as either a graph or as text, depending on your selection.

How to Generate a Report of an Analysis

1. Click the **Report** menu.

2. Click the type of report you want.

3. The results of the analysis are displayed as ASCII text that can be saved, printed, searched, or copied into another application.

More Help

For more information about the Statistical Analyzer, see the online Help.

The Configuration Manager

The Configuration Manager module eases the task of building custom configuration files for modems. You can use it to create as many configuration files as you like, to be applied to individual modems or groups of modems as you require. You can also use it to edit the default configuration file, DEFAULT.CFG.

To run Configuration Manager from Windows, double-click the Configuration Manager icon in the MultiCommManager program group or Start menu. To run it from the Manager, click the **Configuration Manager** button on the toolbar.
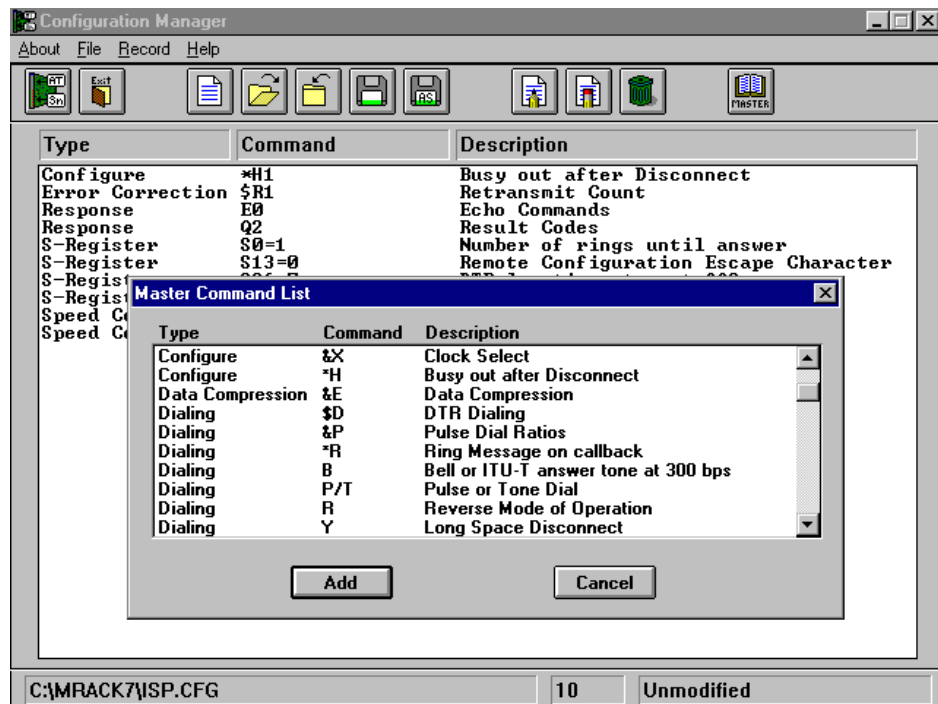
Note: We recommend that you use Configuration Manager only for MultiModemManager rack modems (MR4800 or MR4800E controller). To configure CommPlete Communications Server modems (MR9600 controller—identified as an MR2400 in CC2400 systems), use the RASExpress application.

Configuration File Basics

A configuration file is an ASCII text file with a .CFG extension that contains one or more modem command strings. A command string consists of AT commands and S-register settings that together determine how a modem operates.

Each modem has a complete factory default configuration that is used to initialize the modem. The easiest way to create a custom configuration file is to use only those commands that differ between the factory default configuration and your custom configuration. Commands that do not change can be ignored.

There are two kinds of commands: Master List and user-defined. Master List commands are predefined commands taken from the **Master Command List** dialog box. User-defined commands are created by the user in the **User Defined Command** dialog box. User-defined commands may be required if you want to use commands that are not included in the **Master Command List**, if you want to add a comment to a command, or if command order is important.

When you create a configuration file using Configuration Manager, the Master Command List commands that you select are automatically compiled into one or more AT command strings. Your user-defined commands are inserted into the file on separate lines.

Configuration File Procedures

MultiCommManager resets a modem to the factory default configuration before it sends a new configuration to it. In the configuration file, list only those commands that differ from the factory default configuration. For example, if the factory default configuration has compression enabled (**&E15**) and the only change is to disable it (**&E14**), include only the **&E14** command in the configuration file.

How to Create or Edit a Configuration File

1. Start Configuration Manager.

2. Click **File|New** to create a new configuration file or click **File|Open** to edit an existing configuration file.

3. Click **Record|Master List** to open the **Master Command List** dialog box.

4. In the **Master Command List** dialog box, double-click the commands you want to add to the configuration file, and select the parameter you want for each.

5. To add a command that is not in the **Master Command List** dialog box, click **Record|Add** and type the command and description in the **User Defined Command** dialog box. If the

order of the commands is important, add them in the order in which you want them to be processed.

6. To change the parameter of an existing command, double-click it.

7. To delete a command, select it and click **Record|Delete**.

8. When you are done, click **File|Close** or **File|Save As** to save the file and close it.

How to Send a Configuration File to a Remote Rack

Use the following procedure only for MultiModemManager rack modems (MR4800E controller). To configure CommPlete Communications Server modems (MR9600 controller), use the RASExpress application.

1. Create the configuration file in Configuration Manager.

2. FTP to the controller of the remote rack.

3. FTP the .CFG file from the MultiCommManager supervisor console to the A:\MMM\ directory of the remote controller.

More Help

For more about the Configuration Manager and configuring modems, see Chapter 4, "Organizing and Configuring Your Modems," and the online Help.

The Security Database Editor

The Security Database Editor module can help you create and maintain a callback security database for your system. It offers multilevel security for systems that do not use security servers, and provides flexibility with simple operation for both the system administrator and the dial-in user.

Callback security uses a security database to screen callers. The database contains records of user IDs with (typically) the user's full name, the security status of the user (enabled or disabled), the valid access dates and times for the user, and the type of callback security established for the user (pass-through, fixed callback, or variable callback). You can create as many databases as you have space on the management workstation's hard disk.

Before you set up your security database, you must use the **Setup|Modem| General** command in the Manager to select which modems in your system are to accept inbound security calls and which modems are to be used to call back, if callback is needed.

To run the Security Database Editor from Windows, double-click the Security Database icon in the MultiCommManager program group or Start menu. To run it from the Manager, click the **Security Database Editor** button on the toolbar.

Note: The Security Database Editor is for MultiModemManager sites only. It does not apply to CommPlete Communications Server sites, which should use RADIUS or TACACS+ security.

Security Database Procedures

How to Create a Template

A template is a partly filled-in database record that can save steps when creating a database and ensure that your user profiles are set up in a consistent manner. Before entering users into a new database, you should separate them into different classes based on security level and type, and create a template for each class.

To create a template

1. Open the Security Database Editor.

2. Click **Edit|Set Template**.

3. In the **Set Template** dialog box, click **Add**.

4. In the **Enter Name** dialog box, type a name for the template and click **OK**. The Template dialog box appears with all record fields available except the **Name**, **User ID**, and **Password** fields.

5. Enter only information that will be common to all user records to which this template will be applied.

6. Click **OK** when you are finished. The template name appears in the template list of the **Set Template** dialog box.

7. Click **Done** to exit the **Set Template** dialog box.

How to Create a Database

1. Open the Security Database Editor.

2. Click **File|New**.

3. Click **File|Save As**, type a name for the database file, and click **OK**.

4. In the **Enter New Password** dialog box, type a password for the database, then retype it to confirm it and click **OK**.

5. To add a user to the database, select **Record|Add**.

6. In the **Record|Add** submenu, select a template for the record.

7. In the **Edit/Add Database Entry** dialog box, enter the user name, ID, password, and any individual options that are not already set by the template. (If you want, you can override the template settings.) If you have multiple security modem groups, pay particular attention to setting up which modem groups the user belongs to.

8. When you are done, click **OK** to save the record and exit the dialog box. The record appears in the database window of the Security Database Editor.

9. Repeat steps 5–8 several times to create more records.

10. Select **File|Save** to save the database.

11. Click **File|Exit** to close the Security Database Editor.

12. Test your system and make sure it is functioning properly, then add the rest of your users.

More Help

For more information on how to use the Security Database Editor, refer to Help. For more information about security issues, see Chapter 5, "Security."

4 Organizing and Configuring Your Modems

Organizing Your Modems

The primary purpose of the Explorer is to organize your modems so that they are easier to manage. The physical view shows the physical organization of your modems, whereas the logical view shows the logical organization of your modems. The basic unit of organization in each window is the group.

To organize your groups, you can drag objects to and from them. In the logical view, you can drag both racks and modems (when you drag a rack, you are really dragging the modems that are in the rack). In the physical view you can drag only racks (modems always appear under the rack in which they are physically installed), and then only for local sites. For remote sites in the physical view, groups are predefined.

Rack Groups

Rack groups show the physical organization of your racks and modems. Organizing your racks into groups allows you to organize them by physical location. For example, you might create the following rack groups: Sales Wiring Closet, Purchasing Wiring Closet, and Administration Wiring Closet to indicate where the racks are located.

Note: CommPlete Communications Server rack groups are predefined and cannot be changed, renamed, or moved.

Modem Groups

Modem groups allow you to organize your modems functionally or by any other criteria you choose. An advantage of functional organization is that it allows modem attributes to be set by group.

Click a modem group that you have created and then click **Edit**. In the **Edit Modem Group** dialog box are options that can be set for the modems in the group, such as when the modems get configured and whether modem events are saved to the event file. You can also use modem groups to determine which modems users can call into and get called back from.

See also: "Configuring Your Modems" on page 27.

Organization Procedures

How to Create a Rack or Modem Group

Note: Rack groups are predefined at a Complete Communications Server site.

1. In the Explorer, click the IP site to which you want to add a group.

2. Click **Add**.

3. Type the group name and, optionally, the name and phone number of the contact person for the group.

4. Click **OK.**

How to Move a Rack Between Groups

1. In the logical view of the Explorer, double-click the IP site to display the modem groups.

2. Display the racks in the source group by double-clicking it.

3. Using your mouse, select the rack you want to move and drag it from the source group to the destination group.

How to Move a Modem between Modem Groups

1. In the logical view of the Explorer, double-click the IP site to display the modem groups.

2. Double-click the source group to display your racks.

3. Double-click the source rack to display the modems in the rack.

4. Select a modem and drag it from the source group to the destination group. The rack that the modem is physically located in will appear above the modem in the destination group. To select and move more than one modem at a time, you must hold down the SHIFT key during the move.

Note: In the logical view, the same rack can appear under more than one modem group.

Configuring Your Modems

The MultiCommManager system is configurable and can be adapted to many different computing environments. Two types of modem parameters can be configured: AT commands and **Modem General Setup** settings. Also, the condition upon which a configuration is sent to the modems can be set by modem group.

The AT commands that are configured are the same commands that can be sent to the modem through the modem's serial port. The actual AT commands that are sent depend on the intended purpose of the modem and the modem model; some newer modem cards have different command sets than older models. AT commands can be grouped together in a modem configuration file that can be used to configure modems used for similar purposes. E.g., the configuration file UNIX.CFG could contain all the commands required by modems attached to a UNIX system. These files can be created and edited by Configuration Manager. It is important to note that when these sets of AT commands are sent to the modem, the modem is set first to the factory default settings, so the configuration files need only contain differences from the modem's factory default setting.

Modem General Setup settings include options that might be set by switches on the modem, such as whether the modem is to be a dial-up or leased-line, asynchronous or synchronous, security or non-security modem. **Modem General Setup** cannot be configured at a CommPlete Communications Server site.

Configuration Planning

When configuring a MultiCommManager system, you may find it useful to ask yourself the following questions.

Are your modems connected to one type of host device or to multiple types of host devices?

The host device is the device that is connected to the serial port of the modem. Examples of different types of host devices might be a UNIX system, an AS/400 system, a terminal server, a remote node gateway, a fax server, etc. Different types of hosts can require different modem configuration files and different **Modem General Setup** settings, because different hosts can expect the modem to perform in different ways. It helps to put modems that are connected to the same type of host in the same modem group, so the **Configuration Options** settings in the **Edit Modem Group** dialog box can be set the same for the modems. Examples:

Host 1

A RASExpress server or a fax server needs no configuration because it reconfigures the modem before and after every call.

Modem configuration file:
DEFAULT.CFG (not used)

Modem General Setup *settings:*
Asynchronous(default)
Dial-up (default)
None

Configuration Options *settings for modem group Fax Server:*
None (the fax server takes care of it).

Host 2

A UNIX system requires no responses from the modem unless given a command from the UNIX system, and requires the serial port to be set to 19200 bps. Inbound security is required.

Modem configuration file:
Q2 (for quiet answer settings)
$SB19200 (for a serial port speed of 19200 bps)

Modem General Setup *settings:*

Asynchronous (default)
Dial-up (default)
Inbound

Configuration Options settings for modem group UNIX:

On Disconnect (to make sure the modems are reconfigured after every call).
On Rack Power Up (to make sure the modems are reconfigured after the card is installed).

See also:
- "How to Move a Modem Between Modem Groups" on page 27.
- "How to Create or Edit Modem Configuration Files" on page 31.
- "How to Assign Configuration Files to Modems" on page 32.
- "How to Set Modem General Setup settings for Modems" on page 32.
- "How to Set Modem Group Configuration Settings" on page 33.

Are all the modems of the same type?

Modems are available for the MR4800 rack that meet two different standards: the MT1432MR, a V.32bis modem with V.17 fax capabilities, and the MT2834MR/MR6, a V.34 modem with V.17 fax capabilities. AT commands that apply to one of these may not apply to the other. For example, an MT2834MR/MR6 can be set with a modem baud rate of 28,800 bps by the command **$MB28800**, but the MT1432MR would give an error to this command. Because different modems may require different configuration files, you may want to put all modems of one type into one modem group and all modems of another type into another modem group.

See also:
- "How to Move a Modem between Modem Groups" on page 27.
- "How to Create or Edit Modem Configuration Files" on page 31.
- "How to Assign Configuration Files to Modems" on page 32.

Does the host system configure the modem?

Some host devices such as fax servers might initialize the modem before and after every call, whereas other devices such as a terminal server might never configure the modem. If the host does not configure the modem, then MultiCommManager probably should. If the host does configure the modem, then MultiCommManager must not. If both the host and MultiCommManager try to configure the modem at the same time, the host will error out because the modem ignores all input from its serial port while the MultiCommManager is configuring the modem. Host systems that configure the modem could be put into one modem group and host systems that don't could be put into another.

See also:

- "How to Move a Modem between Modem Groups" on page 27.
- "How to Set Modem Group Configuration Settings" on page 33.

What types of phone lines are the modems connected to?

There are two basic types of analog phone lines: leased lines (two-wire and four-wire) and dial-up lines. CommPlete Communications Servers have only digital T1 or ISDN PRI termination.

Leased-lines are always connected directly at both ends, so the modems must be configured for leased-line operation by setting the **Modem General Setup** settings to **2-wire Leased Line** or **4-wire Leased Line** as required. You also must set the modem to **Answer** or **Originate**, whichever is the opposite of what the modem on the other end is set to. Some modems can be connected to both a leased line and a dial-up line, so that if the leased line fails and the modem is set to **Dial-Backup**, it will call the other modem on the dial-up line to reestablish the connection.

Note: Make sure that the modem group the leased line modem is in is set to configure the modem on reset and disconnect. This is because if the leased line drops or the modem is reset, it will not try to reestablish the connection until it is configured again.

Dial-up lines on host systems used for inbound calls are usually put into some sort of call pool. That is, one phone number may be used to call a group of phone lines (which are connected to a group of modems). When the phone number is called, the first non-busy line is used to handle the incoming call. Modems that are connected to such a call distribution should be set out-of-service (go off-hook) when the device connected to its serial port is inactive. This ensures that incoming calls will not roll over to this inactive device. One way to do this is to set up the S36 and S37 registers in the modem configuration file so that when DTR is not high, the modem will automatically go out-of-service. See the ISP.TXT file in the MRACK directory or folder.

See also:

- "How to Move a Modem between Modem Groups" on page 27.
- "How to Set Modem Group Configuration Settings" on page 33.
- "How to Set Modem General Setup settings for Modems" on page 32.

Configuration Procedures

How to Create or Edit Modem Configuration Files

Use the Configuration Manager to create and edit modem configuration files. (You can access it by either double-clicking the Configuration Manager icon in the MultiCommManager group, or by

clicking the **Configuration Manager** button on the right side of the Manager toolbar.) Create only one configuration file for each type of configuration that you need. The configuration type could be based on the type of modem, the type of host to which the modem is connected, the firmware level that the modem is running, or other considerations. Do not create one configuration file per modem.

Configuration files should include only commands that are different from the factory default settings of the modem. Items that should be considered when creating modem configuration files are the serial speed at which the host expects to talk to the modem, the types of error correction and data compression that are desired, and the RS-232 signaling requirements that your host device has.

See also: "How to Assign Configuration Files to Modems" on page 32.

How to Select Modems

Modems can be selected in different ways depending on which window is active. For the Explorer window, when an item is selected, everything underneath it in the hierarchy is also selected. For instance, if you select an IP site, then all the modems at that IP site are selected; if you select a modem group, then all modems in the group are selected; etc. In the rack display window, a modem can be selected by clicking the button associated with the modem (A–H). In the modem status window, the modem that is shown is automatically selected.

How to Assign Configuration Files to Modems

1. In the Manager module, select the modems to which you wish to assign a configuration file.

2. Click **Setup|Modem|Configuration File**.

3. In the dialog box that appears, select a previously created configuration file.

See also: "How to Select Modems" on page 32.

How to Set Modem General Setup Settings for Modems

Note: Does not apply to CommPlete Communications Server sites.

1. In the Manager module, select the modems whose **Modem General Setup** information you want to set.

2. Click **Setup|Modem|General**.

3. In the **Modem General Setup** dialog box, select the options you want.

See also: "How to Select Modems" on page 32.

How to Set Modem Group Configuration Options

1. In the Explorer, open the IP site containing the modem group whose settings you wish to change.

2. Click the modem group.

3. Click the **Edit** button.

4. In the **Edit Modem Group** dialog box, select the **Configuration Options** you want.

5. Click **OK** to close the dialog box.

5 Security

Introduction

Note: This chapter does not apply to CommPlete Communications Server sites (HD8 modems), which use RADIUS and TACACS+ for security.

MultiCommManager can provide an additional layer of security between your users and your system. It can prompt users for a user ID and a password when they call in. If they pass that security check, it can either connect them directly to the system or call them back, either at a fixed or a changeable number, and log them in. It can let users in only at certain times of day, certain days of the week, or only between certain dates. Also, it can require users to change their passwords after a certain interval of time.

Access to security modems attached to particular hosts can be controlled by making users members of particular modem groups. Also, callback users can be prompted for which host (i.e., which modem group) will call them back if the host select feature is enabled.

Callback Security

When a modem receives a call, the modem prompts the user for the assigned user ID and password. This login information is sent to the control PC from the rack controller. The control PC verifies the user's login information. If the user ID or password is invalid, the control PC instructs the system modem to prompt the user to enter the information again. If the user reaches the retry limit, the line is disconnected and a fault is logged..

If the user ID and password are valid, and the user is in the security database as a pass-through user, then a message is displayed to the user that the user is now connected to the host system. If the user is a fixed callback user, then the user is placed in a queue at the control PC to be called back after the callback timer has expired and a callback modem is free. If the user is a variable callback user, then the user is prompted for a number to be called back at. After the user the number, the user is placed in the same callback queue as the fixed callback users.

Each entry in the callback queue waits the number of seconds specified by the callback timer before attempting to get a free callback modem to dial with. When a free modem is available, the modem dials the number in the security record if it is a fixed callback, or the number entered by the user if it is a variable callback (if the variable callback user presses ENTER instead of typing a number, the number in the user's security record is used). If the number being called back is busy, or a connection is not made, the entry is set to be retried after the number of seconds specified by the callback timer. If callback fails after three retries, the entry is deleted from the queue. If the connection is made, then the user is connected directly to the host.

Callback Types

- **Pass-through:** Uses only user ID and password verification.

- **Fixed callback:** Uses a fixed, predefined callback phone number from the Callback Security database after user ID and password verification.

- **Variable callback:** Uses either a callback phone number entered by the user, or a fixed, predefined callback phone number from the callback security database after user ID and password verification.

Security Types

- **Pass-through:** This type of security requires a user to perform a normal login procedure (that is, to provide his or her user ID and password) before access to the host is permitted. The user is given a preset number of login attempts, which the system administrator sets in the **Security Defaults** dialog box. If a user is unsuccessful, the line is disconnected and a fault event is recorded. This eliminates the possibility of a hacker, randomly generating passwords, to have adequate time to chance upon a valid password.

- **Fixed callback:** This type of security requires a user to perform a normal login procedure (that is, to provide his or her user ID and password) before access to the host is permitted. The user is given a preset number of login attempts, which the system administrator sets in the **Security Defaults** dialog box. The system then disconnects and calls back the user at the callback phone number listed in the security database. A hacker who has managed to obtain a legitimate password and user ID would not be able to gain access to the system because he or she would not be at the legitimate callback number.

- **Variable callback:** This is the most useful type of security for your frequent travelers or laptop users, such as sales representatives, claims agents, and repair technicians. This method works like fixed callback, except that the user is prompted for the callback phone number at his or her *present* location. If your user presses ENTER when prompted for the phone number to call back, variable callback assumes that the user is at the fixed callback location, and automatically calls the user at the callback phone number listed in the security database.

Note: You can use the **Callback Blacklist** command to prevent callback to a phone number or a range of numbers. See the online Help.

Security Planning

Your answers to the following questions will help you set up your security configuration.

Do You Need MultiCommManager Security?

Reasons why you may want to use MultiCommManager security:

You have a host that has little or no security for inbound calls

If you have a host device that doesn't provide security, then MultiCommManager can be your security device, providing all of the security options that were detailed in the chapter introduction. Also, even if you have security, MultiCommManager security might provide more features than the built-in security that your host device has. For example, your host device might not be able to screen users by time of day or day of the week.

You would like an extra layer of security

If your system already provides call-in security, MultiCommManager security can provide an additional layer of security of a different type. With MultiCommManager callback security, the person calling in must have physical access to the callback phone in order to get into the system.

You want the company to pay for long-distance calls to a host

MultiCommManager security can provide reversal of phone charges by calling back a user after the user has passed the security check. The user would have to pay for the short call-in security check, but the company would pay for the rest of the time online.

You want to track who is connecting to a host

Using the Call Traffic window, you can tell who is connected into your system at any time. Using the Statistical Analyzer module, you can produce reports that will tell you who was connected to your system, for how long, and when. This information can be used for billing or security purposes.

See also: "How To Set Up Security Modems and Modems Groups" on page 45.

Do You Need Pass-Through, Fixed Callback or Variable Callback Security?

Pass-through, fixed callback, and variable callback are security types that are set on a per-user basis. The following table shows characteristics for each type of security.

Characteristic	Pass-through	Fixed callback	Variable callback
Security level	Lowest	Highest	Middle[1]
User's location	Anywhere	One location	Anywhere
Reverse charges	No	Yes	Yes
Convenience	Highest	Middle	Lowest[2]

[1] If the call-in user gets someone else's user ID and password, you can track the number that was actually called back

[2] The user must enter a phone number if he is at a different callback number than the default.

Example 1

You are using MultiCommManager security primarily to reverse charges for your long distance callers and to track who connects to your system. High security is not an issue.

Long Distance Users: Set to variable callback with a default callback number that doesn't need to be entered every time the users log in.

Local Users: Set to pass-through, since there is no need to reverse charges for them.

Administrator: Set to fixed callback for the highest security level.

Example 2

You are using MultiCommManager security as an extra layer for an extremely secure system.

Traveling Users: Set users at hotels that can't accept direct incoming calls to pass-through, otherwise set them to variable callback. Set them to these security types only while they are traveling; set them back to fixed callback when they return.

Other Users: Set to fixed callback.

Do You Have Multiple Host Types that Users Need to Access?

Having multiple host types is handled in MultiCommManager security by placing modems that are attached to one type of host device, such as a UNIX system, into a common modem group. Users who need access to that host should be made members of that modem group. This ensures that users who connect to modems that are in a modem group that they are not members of will have their user IDs and passwords rejected. Also, it ensures that they will be called back only by modems that are in modem groups that they are members of.

If you want to prompt callback users to select the host that will call them back, you must enable the Host Select feature. When this is active, callback users who are members of more than one modem group that has outbound modems in it are prompted to pick the host that they want to be called back by. The names displayed are the names of the modem groups that they are members of. This feature is not available with pass-through security.

See also: "How to Set Up Security Modems and Modem Groups" on page 45.

Do You Have Multiple Security Levels for Call-In Users?

You may want to give some users, such as system administrators, more access to your system than ordinary users. But the amount of access that you give may also depend on what type of data the users are accessing. If the data is sensitive, then you will probably want to lock out your least trusted users (LTUs) and restrict even your most trusted users (MTUs) so that it would be difficult for anyone to hack into the data. If the data is not sensitive, then your MTUs could be given more freedom and your LTUs could have restricted access. The different access privileges for MTUs accessing your most sensitive data versus your least sensitive data could be accomplished by having a different user account for each type of data for the user (e.g, have an administrative account for doing system maintenance, and a regular account for normal access to the system).

MultiCommManager security has many security barriers that can be adjusted to allow many different security levels. The following table shows the different barriers and how they might be set for different types of users and data.

Security barrier	Possible values (most to least secure)	Most sensitive data	Least sensitive data
Security type	Fixed callback. Variable callback. Pass-through.	Allow only MTU; require access via fixed callback.	Allow MTU freedom with pass-through or variable callback, and LTU restricted access through

			fixed callback.
How often user must change password	Very often to not at all.	Allow only MTU; password should change very often.	Allow MTU long time between password change. Allow LTU access to one of few modem groups.
Number of modems that user can access through modem group member-ships*	Member of some or one modem group. Member of all modem groups.	Allow only MTU; give access to all modem groups because MTU has to access all hosts for maintenance.	Allow MTU access to all modem groups. Allow LTU access to some or one modem group.

Security barrier	Possible values (most to least secure)	Most sensitive data	Least sensitive data
Valid times	No hours for any day of the week to all hours for all days of the week.	Allow MTU access at any time for system maintenance.	Allow MTU access at any time. Allow LTU access only during business hours.
Usage dates	Restricted dates to unrestricted dates.	Allow MTU access on any date for system maintenance.	Allow MTU access on any date. Allow LTU access only for a limited range of dates.
Number of user IDs per user	One per user to several per user.	Give MTU a separate user ID for most sensitive data.	Give MTU a separate user ID. Give LTU only one user ID.

* Some modems attached to a given host type could be put into a special modem group so that even if all the modems are full, an administrator could get into the system on one of those modems. Also, it might be possible for a system to restrict administrator level access only to certain physical ports, which could be in this special modem group.

Example

You have a system that has three different types of hosts. You have one senior administrator who can administer any of the host types and three administrators that can only administer their own

host types, two support technicians that help users with system problems, and normal users. These users are set up as follows:

Senior Administrator: Has two accounts. *Administrator account:* Set to fixed callback, password change every week, member of all modem groups, access at any time, day of the week, and date. *User account:* Set to pass-through, password change every three months, member of all user-accessible modem groups, access at any time, day of the week, and date.

Host Type Administrator: Has two accounts. *Administrator account:* Set to fixed callback, password change every week, member only of modem groups for the host type, access at any time, day of the week, and date. *User account:* Set to variable callback, password change every three months, member of all user-accessible modem groups, access at any time, day of the week, and date.

Support Technician: Has one account only. Set to variable callback, password change every month, member of all user-accessible modem groups, access during business hours only, dates starting and ending as appropriate.

Normal User: Has one account only. Set to fixed callback, password change every month, member only of user-accessible modem groups for host types that access is needed for, access during business hours only, dates starting and ending as appropriate.

See also:
- "How to Set Up Security Modems and Modem Groups" on page 45.
- "How to Set Up Your User Database" on page 46.

Do You Require Users to Change Their Passwords?

By requiring users to change their passwords, you can make sure that if someone learns someone else's password, there is a limited time during which they can get unauthorized access to the system. Users who access the system's most sensitive data should be required to change their passwords often. Least-trusted users should also be required to change their passwords fairly often.

See also:
- "How to Set Up Your User Database" on page 46.
- "How to Set Global Security Attributes" on page 47.

What Days and Times Are Users Allowed Access to the System?

You can restrict the times during the week that a user can access the system down to the hour. Your administrators, who must be able to deal with system problems at any time, should of course be given access at any time of the week. Normal users who would need to access the system only during business hours should be given access only during business hours. Users who are on the road and may be calling in during the evening or weekend could be given access between 6:00 A.M. and 12:00 A.M. Of course, many other possibilities exist.

See also: "How to Set Up Your User Database" on page 46.

What User Interface Do You Want to Present to Call-In Users?

MultiCommManager security allows you to fully configure the messages that are presented to call-in users. You might want to try the default setup first and decide later what you want to change (the welcome message is a common one to change).

See also: "How to Set Up Your Own Security User Interface" on page 47.

Which Modems Should Be Dial-In, Dial-Out, or Both?

MultiCommManager security allows you to set your modems to allow only dial-in calls (inbound security modems), dial-out calls (outbound security modems),or to allow both ("both" security modems). Dial-in modems can be used for either pass-through calls or for the first part of callback calls. Dial-out modems can be used only to call back callback users (the second part of a callback call). "Both" modems can be used to either accept inbound security calls or to call back callback users.

Example 1

Callback only—one host type.

Modems	Security type	Connected to	Modem group
1A–1B	Inbound security	Nothing	Unassigned
1C–1F	Outbound security	The host computer	Unassigned

1A and 1B are not connected to any host on their RS-232 ports. They accept only short inbound calls in which users call in and pass security so that they can be called back.

Example 2

Callback for normal users only, callback and pass-through for administrative users—one host type.

Modems	Security Type	Connected to	Modem Group
1A–1D	Inbound security	Nothing	NormalInbound
1E–3F	Outbound security	The host computer	NormalOutbound
4A–4E	Outbound security	The host computer	AdminOutbound
4F	Inbound security	The host computer	AdminInbound

Normal users are members of the NormalInbound and NormalOutbound modem groups. Administrative users are members of the NormalInbound, NormalOutbound and AdminOutbound groups. This makes sure that even if the all of the normal inbound security modems are in use, an administrative user can still get in on the AdminOutbound group. The senior administrator is a member of the AdminInbound group and is a pass-through user, since that modem will only be used by him or her. All other users are fixed callback.

Example 3

Callback only—three host types (host selection enabled).

Modems	Security Type	Connected to	Modem Group
1A–1B	Inbound security	Nothing	Inbound
1D–1E	Outbound security	UNIX host	UNIX
1F–2D	Outbound security	AS/400 host	AS/400
2E–2F	Inbound security	DEC VAX	VAX

Users are all members of the Inbound modem group. They are also members of the modem groups that correspond to the hosts that they are to have access to. When users who are members of more than one outbound modem group call in, they are presented with a prompt that asks them which host they want to call them back.

Example 4

Pass-through and callback users—one host type.

Modems	Security Type	Connected to	Modem Group
1A–2F	Both security	The host computer	Unassigned

This site has a mix of callback and pass-through users, so the system has to have both dial-in and dial-out security modems. However, separate modems for the pass-through users and the callback users are not desired. By setting all the modems to be "both" security modems, the modems can be shared for both purposes.

See also:

- "How to Set Up Security Modems and Modem Groups" on page 45.
- "How to Set Up Your User Database" on page 46.

Security Procedures

Setting up MultiCommManager security requires some planning before making changes. The following sections will help you set up security for the first time.

How to Set up Security Modems and Modem Groups

1. First decide which modems should be security modems and what modem groups they should be partitioned into, and create modem groups for them. This should reflect your need to control access to different host types and access by users with different security levels. Also consider what type of security modem (inbound, outbound, or both) each modem is going to be.

   Note: Chapter 4, "Organizing Your Modems" explains how to create modem groups and how to put modems into them. If you need only one modem group, then you may want to create a modem group just for your security modems instead of using the Unassigned modem group as your modem group.

2. When the modem groups have been created, click on a modem group to select all the modems in it, and select **Setup| Modem|General** to open the **Modem General Setup** dialog box. Set the security type for all the selected modems.

3. Select **Control|Load Modem Configuration** to update the modems to their new settings as security modems. Repeat this procedure until all of your modem groups have their security type set correctly.

4. If you want your callback users to be able to select the host that calls them back, be sure to enable the Host Selection feature for the site by selecting **Setup| Modem|Security|Host Select** and enabling **Allow Host Select** in the dialog box.

How to Set Up Your User Database

1. Select **Tools|Security Database Editor** to run the Security Database Editor. In the Security Database Editor you can create new security databases or edit existing security databases.

2. Before entering users into the database, separate them into different classes based on security level and type and create a template for each class, so that your user profiles are set up in a consistent manner. To add one user to the database, select **Record|Add.** This opens a dialog box in which you can set up all settings for your user. If you have multiple security modem groups, pay particular attention to setting up which modem groups the user belongs to.

3. After entering a few users, save the database file by selecting **File|Save** and typing a distinctive file name.

4. Test your system and make sure it is functioning properly, then add the rest of your users.

For more information on how to set up a template or use the Security Database Editor, see the online Help.

How to Test or Monitor Your Security System

When a user dials into a security modem, he or she should see a welcome message followed by a user ID prompt. After entering a user ID and password, the user should either be connected directly to the host, if the user is a pass-through user, or get a message saying that the user will be called back, if the user is a callback user. If the user is a variable user, then the user should be prompted for a phone number at which to be called back. If the modem doesn't answer, then it is either an outbound security modem or it hasn't had its settings loaded into it. If the modem answers but displays no prompts then it probably hasn't had its security settings loaded.

If the user is a pass-through user, then you should be able to look in the Call Traffic window to see the connection and which user is connected to the modem. If the user is a callback user, you should be able to see the user in the Callback Queue window. Here you can watch the modem as it tries to call back the user. Once the user is called back and the connection is made, the user disappears from the Callback Queue window and appears in the Call Traffic window.

How to Set Global Security Attributes

MultiCommManager security has several global parameters that can be modified, such as whether users should be prompted for passwords and how many times a user can fail a user ID/password security check before the call is disconnected. You can modify these settings by selecting **Setup|Modem| Security|Defaults**.

How to Set Up Your Own Security User Interface

MultiCommManager Security allows you to customize the messages that are displayed to users when they call into a security modem. You can edit or replace the default security messages by selecting **Setup|Modem|Security| Messages**. In these messages, carriage returns are represented by **^M**, and line feeds by **^J**.

How to Set Up Which Database Files Are Active

MultiCommManager security allows multiple security database files to be active at one time, so that whole sets of users can be enabled or disabled at once. For example, by putting an entire class of students at a university in one database file, you can disallow graduated students access to the system by deactivating the database file. You can change which database files are currently active by selecting **Setup|Modem|Security| Database Files**.

How to Set Up a Global Variable Callback Number Blacklist

MultiCommManager security allows you to have a global blacklist of phone numbers and classes of phone numbers that will be rejected when entered as a variable callback number. You can reject classes of phone numbers by the use of wild card symbols. For example, **612*** rejects all phone numbers with a 612 area code. You can edit the blacklist by selecting **Setup|Modem|Security|Phone Number Blacklist**.

6 Monitoring and Controlling Your System

Monitoring Your System

The following sections describe how to monitor your system using the different views available in MultiCommManager. For more information see the online Help.

Fault and Status Events Window
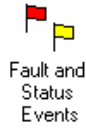
To display the Fault and Status Events window, click **View|Faults/Status** or double-click the Fault and Status Events icon in the client area of the main window. This window cannot be closed.
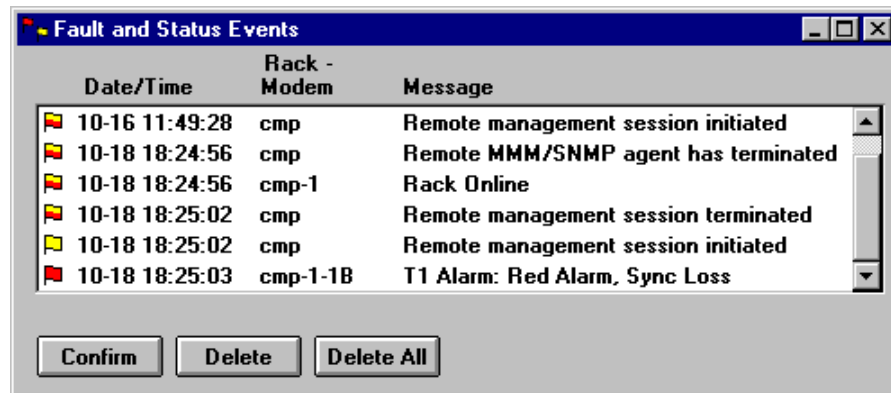
Use the Fault and Status Events window to alert you if something goes wrong in your MultiCommManager system. Two types of events appear in this window: serious problems, or faults, which are flagged with a red flag, and status events, which are flagged with a yellow flag. Keep a close eye on this window and either confirm events (which turns the flag red and yellow), or delete them to make it easier to see when something goes wrong.

If you are using the Fault and Status Events window on a supervisor node, modems that have a fault or status event at other IP sites are identified by a three-letter site name (the IP site's short name), the rack number, and the modem ID. For example, CMP-1-1B identifies site CMP, rack 1 and modem 1B.

See also:
- "How to Edit an IP Site" on page 13.
- Online Help

Call Traffic Window

To display the Call Traffic window for an IP site, select an IP site in the Explorer and click the **Display** button. To display the Call Traffic window for the local site, click **View|Call Traffic**. To display a minimized Call Traffic window, double-click the Call Traffic icon in the client area of the main window.

Call Traffic

You can use the Call Traffic window to display a history of your system's modem connections up to the last 200 calls—for a longer period, use the Statistical Analyzer. At any time during the day, some of your modems will be connected, answering a call, originating a call, or sitting idle. Here you can see which modems are in which of the first three states, and if the call was originated, which number was dialed, and if the call was completed, for how long it was connected.

The Call Traffic window also allows you to determine who is using what modem. If you are using MultiCommManager security, the user ID of the user is listed along with the modem that the user is connected to. If you are using MultiCommManager with RASExpress, you can see who is using the modem for outbound use.

If you are using MultiCommManager with SNMP, you can display a separate Call Traffic window for each IP site. The title bar contains the IP site's long name.

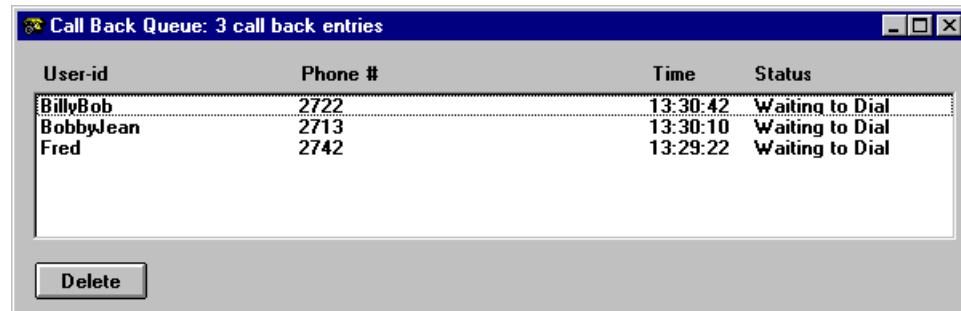For more information see the Online Help.

Call Back Queue Window

To display the Call Back Queue window, click **View|Callback Queue** or double-click the Callback Queue icon in the client area of the main window.

Note: This window is not used with CommPlete Communications Server modems.


This window is used with MultiCommManager security. It shows which users have passed security and are either responding to further modem prompts, or are waiting to be called back. This is a good debugging tool if you are trying to get your MultiCommManager security up and running.

For more information see the online Help.

Rack Display Window

To open the rack display window, click a rack icon in the Explorer and then click **Display**.
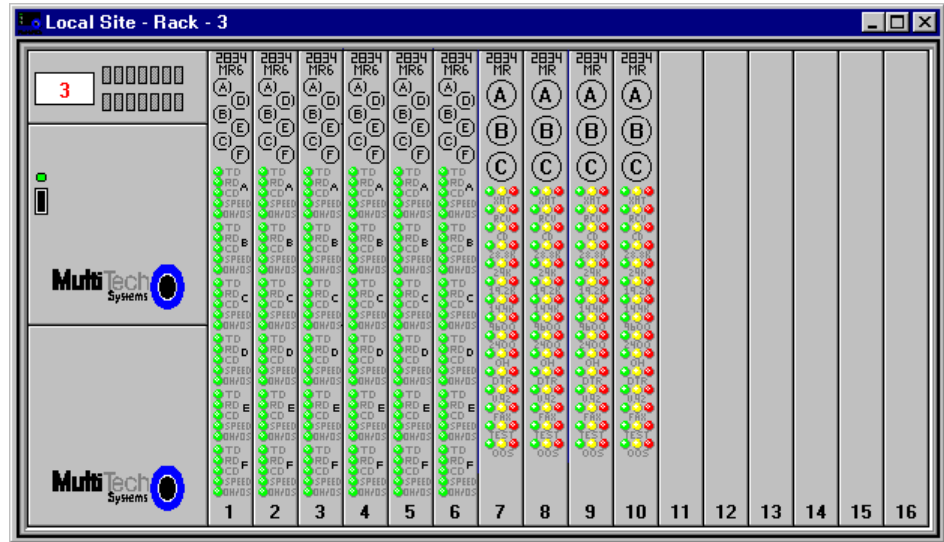
This window shows a graphic display of a rack. It shows which modem cards are installed, which power supplies are installed and operating, and the node ID of the rack. (Note, however, that the LED states in this display are for purposes of illustration only.) From here you can select modems to manage. If you click the **Toggle Full Rack Display** button, the display changes to show the current status of all installed modems.

For more information see the online Help.

Modem Status Window

You can display a modem status window by any of three methods:

- Click on a modem icon in the Explorer and then click **Display**.
- Double-click on a modem icon in the Explorer.
- Double-click on a modem button in a rack display window.
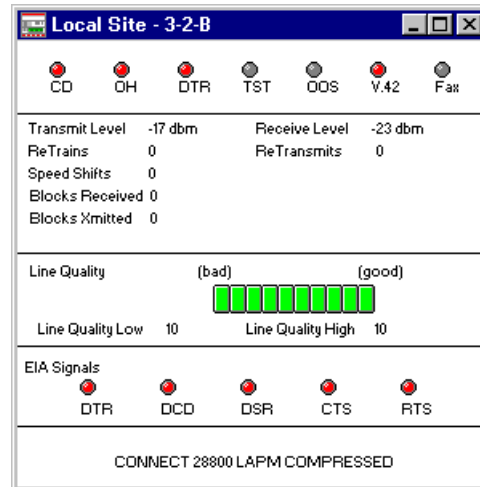
This window shows in-depth information about a single modem. It accurately shows the state of the modem's LEDs. When the modem is connected, the window displays a number of online statistics, including a graphic view of the line quality and a text view of other online information.

For further information see online Help.

Controlling Your System

MultiCommManager allows you to perform many actions on your system's modems. To perform an action on one or more modems, first select the modems, then select a command.

Select a command by choosing a menu item or its corresponding toolbar button, if it has one. When a command is selected, the current window is asked to give the command a list of its currently selected modems so that the action can be performed on each one.

See also: "How to Select Modems" on page 32.

Configuring Modems

See "Configuring Your Modems" on page 27 and "How to Configure Modems" on page 56.

Testing Modems

A variety of loopback tests can be performed on MultiModemManager legacy link modems in answer and originate modes and at different speeds. These tests make sure that the DSP, the processor, the RAM, and the ROM are all working for the selected modem and speed. They test basically all the hardware except the DAA (data access arrangement), which is the circuitry that connects the modem to the phone line.

See also: "How To Test Modems" on page 57.

Resetting Modems

You can reset a modem to clear it from a stuck state, to hang it up (though you should try **Control|Hangup Device** first), or so that it can be flash programmed from the serial port (this should also work without resetting the modem first). Modems can be reset directly by the system manager or indirectly by letting the MultiCommManager reset modems in response to an abnormal event (to see how to configure this, see "Acting in Response to Faults").

See also: "How To Reset Modems" on page 57.

Hanging Up Modems

You might want to hang up a modem for several reasons: to kick an overtime user off your system (this can also be done automatically by a fault alarm), to free up a modem for an expected call, etc. If the hangup action doesn't work, then try resetting the modem.

See also: "How To Hang Up Modems" on page 57.

Acting in Response to Faults

The MultiCommManager can detect and respond to many faults. Most faults have a programmable threshold which sets how many times an event must occur before an action is performed to deal with it. Depending on the fault, a modem can be reset or re-sent the modem configuration file (in hopes of clearing up the faulty modem), set out of service (so that the other users can't use the modem until the system administrator can deal with the problem), or hang up (so that the modem is available to other users). In addition to the above actions, a pager can be dialed with information identifying the fault.

See also: "How To Set Up Fault Actions" on page 57.

Modem Control Procedures

How To Configure Modems

To configure a group of modems, first select a modem group, then select either
Setup|Modem|General or **Setup|Modem|Configuration File**. Select the appropriate settings in the dialog box and then click **OK**. With the modems still selected, load these configurations into the modems by selecting **Control|Load Modem Configuration**. Until you load the new configuration or an event causes the configuration to be loaded (such as when a modem group has **Configuration On Modem Reset** selected) the modem is not configured with the new settings.

See also:
- "How to Select Modems" on page 32.
- "How to Create or Edit Modem Configuration Files" on page 31.

How To Test Modems

You can test MultiModemManager legacy link modems by first selecting the modem and then selecting the test to be run from the **Control|Test Device| Modem** menu. The test results are displayed on the screen.

See also: "How to Select Modems" on page 32.

How To Reset Modems

To reset a modem, first select the modem in the Explorer and then select **Control|Reset Device**.

See also: "How to Select Modems" on page 32.

How To Hang Up Modems

To hang up a modem, first select the modem in the Explorer, then select **Control|Hangup Device**.

See also: "How to Select Modems" on page 32.

How To Set Up Fault Actions

To set up a fault action on an independent or agent node, click **Setup|Faults and Alarms**. To set up a fault action on a supervisor node, click an IP site in the Rack Groups or Modem Groups window before selecting the **Setup|Faults and Alarms** command.

To edit a fault action, double-click on the fault in the **Faults and Alarms** dialog box. This opens a dialog box that allows you to enable or disable the fault and to select the action associated with it.

7 Solving Problems

Introduction

This chapter provides information that can be used to identify and fix problems with the MultiCommManager system. Problems can be observed at the rack front panel (LEDs, seven-segment display), the management PC's screen, or via audio alarm or alarm report. In addition, problems can be found when performing the diagnostic tests documented in this chapter.

For specific MultiModem troubleshooting information, refer to the modem card user guide. For basic Windows messages, refer to your Windows manuals or Help screens.

POST (Power On Self Test)

When rack power is applied, a self-test is performed to exercise front panel elements. Refer to the rack user guide for further information.

MultiModemManager Link Problems

I can't see my local racks

Check the settings on your MultiModemManager MIC (link) card.

1. Make sure that the IRQ, shared memory address, and I/O addresses are available for the MultiModemManager link card. A good way to do this is to remove the card from your PC and in Windows 3.x run MSD (the Microsoft diagnostics tool). In Windows 95 select **My Computer|Control Panel|System|Device Manager|Computer|Properties**. This will tell you which of these resources are available for use. Even after checking, you may have to try different combinations of the above settings.

2. Make sure that the Node ID switch, which is accessible through the back of the computer, is set to all switches closed (Node ID 255). If your computer is a PS/2, make sure that the Node ID is set to 255 on the Reference Diskette.

3. Make sure that **Setup|Legacy Management|Broadcast Local Racks** is selected.

4. Make sure there is an MultiModemManager link terminator in the last rack of the daisy chain.

5.   If you have more than 4 racks, then you must have a MultiModemManager link hub.

SNMP Problems

I can't see my remote MultiCommManager agent sites

Make sure you defined your managed agents in MultiCommManager.

I can see my remote MultiCommManager agent sites, but they are grayed

1.   Ping the grayed agent site to make sure that it is up and operational.

2.   Make sure that the GET and SET Community strings you specified when defining the agent site in MultiCommManager match those set on the agent site.

3.   Make sure that the SNMP mode on the MultiCommManager agent site is set to **Agent**. The MultiCommManager supervisor cannot recognize remote sites whose SNMP mode is **Independent**.

I never see remote MultiCommManager agent fault/status information

If the MultiCommManager agent site is grayed on the supervisor, follow the preceding troubleshooting steps.

The Call Traffic window or a Modem Status window for a MultiCommManager agent site receives no information

If the MultiCommManager agent site is grayed on the supervisor, follow the preceding troubleshooting steps.

Fault and Status Messages

The following messages can be displayed in the Fault-Status window, in fault reports, or in the log report. A subset of these messages can be found in fault alarm message boxes.

The Fault Analysis Report (Appendix A) provides a set of possible fault reasons. Listed below are the descriptions and remedies for each fault reason.

Arcnet Error Controller may be down

Meaning: The Manager is unable to communicate with the controller.

Recovery: Make sure that the controller is not powered down, and that the connection between the Manager and the controller has not been broken. If neither is the case, restart Windows and the Manager.

Arcnet Send Error During Broadcast

Meaning: The Manager was unable to communicate with one or more controllers during a broadcast message.

Recovery: Make sure that the controller is not powered down, and that the connection between the Manager and the controller has not been broken. If neither is the case, restart Windows and the Manager.

Attempt to use Black Listed Phone Number

Meaning: An attempt was made to enter a phone number in the list of illegal phone numbers. The number falls into a range of blacklisted phone numbers.

Recovery: Remove the number from the black list. Change the wild card list.

Bad Password by user

Meaning: The password entered for the user was invalid.

Recovery: Verify or reset the user password.

Bad UserID

Meaning: An invalid user ID was entered at the user ID prompt.

Recovery: Verify that the user ID is in the data base (case sensitive).

Callback attempt failed

Meaning: This fault is usually associated with another fault that detects why the callback attempt failed.

Recovery: Attempts will be made again until the retry limit is reached.

Congested Rack

Meaning: A predefined percentage of the modems are online.

Recovery: Raise the threshold; add more modems.

Entry Disabled for user

Meaning: The user ID exists, but has not been enabled, or the user ID is not valid at the time the time the request is made.

Recovery: Verify that the user ID is in the database, enabled, and valid for the requested time (case sensitive).

Exceeded Maximum Number of Callback Attempts

Meaning: The callback was attempted the defined number of times, but failed.

Recovery: The modem to call back may have been busy. (Each previous callback attempt ended with a fault report.)

Modem card Installed

Meaning: The controller has been rebooted or powered up; the rack card has been seated or reseated.

Recovery: The controller can be rebooted from the Manager. The modem card screw should be tightened to prevent the modem card from momentarily loosing contact with the backplane.

Modem card Removed

Meaning: The controller was powered down; the modem card was unseated from the rack.

Recovery: The controller can be rebooted from the Manager. The modem card screw should be tightened to prevent the modem card from momentarily losing contact with the backplane.

Modem reset by rack controller card

Meaning: The modem was reset from the Manager.

Recovery: None. This is a status report for an intervention by the operator.

No activity on the Line

Meaning: The modem is connected, but no actual data transfer is taking place. The modem inactivity timer has expired.

Recovery: The inactivity timer is controlled via a modem register.

No Connect - No Carrier/Unable to train

Meaning: No connect.

Recovery: Make sure the carrier is present and line quality is adequate.

No Connect - Probable Wrong Number/Busy

Meaning: The answering phone did not go off hook.

Recovery: Call again later.

No Dialtone - Probable faulty line

Meaning: The outbound call did not receive a dial tone.

Recovery: Verify that the phone line is plugged in and functioning properly.

No Free modem for Callback

Meaning: There were no outbound modems available to use for callback.

Recovery: Change some inbound modems to outbound modems; add more modem cards.

Overtime Call

Meaning: A connection exceeded or continues to exceed the defined threshold for the maximum number of minutes to be online.

Recovery: Reset the overtime call threshold, or break the connection and call again.

Power Supply failure

Meaning: A power supply has failed or has been switched off.

Recovery: No immediate action required if there is a redundant power supply installed.

Rack Online

Meaning: The controller informed the Manager that it has come on line.

Recovery: None.

Ring Detected during Outbound

Meaning: The call was not attempted because a ring was detected by a modem allocated for callback.

Recovery: Retry.

Server Error

Meaning: A command sent from the Manager was not acknowledged.

Recovery: If the problem persists, try exit Windows and restart MultiCommManager.

Test 0:	**ANLB @14400**	**FAILED**
Test 1:	**ANLB @9600**	**FAILED**
Test 2:	**ANLB @2400 Answer**	**FAILED**
Test 3:	**ANLB @2400 Originate**	**FAILED**
Test 4:	**ANLB @1200 Answer**	**FAILED**
Test 5:	**ANLB @1200 Originate**	**FAILED**

Meaning: May indicate a problem with the modem.

Recovery: If the test consistently fails, replace or repair the modem.

Timeout at Password prompt

Meaning: The modem failed to receive a password response within the timeout period (30 seconds).

Recovery: None.

Timeout at UserID prompt

Meaning: The modem failed to receive a user ID within the timeout period (30 seconds).

Recovery: None.

Diagnostic Tests

The resident tests in the MultiCommManager system provide analog loopback (ANLB) tests at the various modem speeds. When you select a test and specify the modems to be tested, the test runs automatically. The system software sends the specified test command to the selected modems and displays a message that indicates whether the test passed or failed for a particular modem.

For more information, see the online Help.

8 Warranty, Service, and Technical Support

Limited Warranty

Multi-Tech Systems, Inc. ("MTS") warrants that this product will be free from defects in material or workmanship for a period of two years from the date of purchase, or, if proof of purchase is not provided, two years from date of shipment.

MTS MAKES NO OTHER WARRANTY, EXPRESSED OR IMPLIED, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED.

This warranty does not apply to any products which have been damaged by lightning storms, water, or power surges or which have been neglected, altered, abused, used for a purpose other than the one for which they were manufactured, repaired by the customer or any party without MTS's written authorization, or used in any manner inconsistent with MTS's instructions.

MTS's entire obligation under this warranty shall be limited (at MTS's option) to repair or replacement of any products which prove to be defective within the warranty period, or, at MTS's option, issuance of a refund of the purchase price. Defective products must be returned by Customer to MTS's factory, transportation prepaid.

MTS WILL NOT BE LIABLE FOR CONSEQUENTIAL DAMAGES AND UNDER NO CIRCUMSTANCES WILL ITS LIABILITY EXCEED THE PURCHASE PRICE FOR DEFECTIVE PRODUCTS.

Technical Support

Multi-Tech has an excellent staff of technical support personnel available to help you get the most out of your Multi-Tech product. If you have any questions about the operation of this product, please call (800) 972-2439 (USA and Canada) or (612) 785-3500 (local and international).

The Multi-Tech BBS

Multi-Tech maintains a bulletin board system (BBS) for its customers. Information available from the BBS includes new product information, product upgrade data, and problem-solving tips. There is also a message service that lets you request additional information. The phone number for the Multi-Tech BBS is (800) 392-2432 (USA and Canada) or (612) 785-3702 (local and international).

The BBS can be accessed by any asynchronous modem operating at 1200 bps to 33,600 bps at a setting of 8 bits, no parity, and 1 stop bit (8-N-1).

Logging onto the Multi-Tech BBS

To log on to the Multi-Tech BBS, perform the following steps:

1.   Set your communications program to **8-N-1**.

2.   Dial our BBS at (800) 392-2432 (USA and Canada) or (612) 785-3702 (international and local).

3.   At the prompts, type your first name, last name, and password; then press ENTER. If you are a first time caller, the BBS will ask if your name is spelled correctly. If you answer yes, a questionnaire will appear. You must complete the questionnaire to use the BBS on your first call.

4.   Press ENTER until the Main Menu appears. From the Main Menu you have access to three main areas: the Files Menu, the Message Menu, and Bulletins. For help on menu commands, type **?**.

Downloading a File

If you know the file name

1.   From the Main Menu, type **F** to access the Files Menu, then type **D**.

2.   Enter the name of the file you wish to download from the BBS.

3.   If a password is required, enter the password.

4.   Answer **Y** or **N** to the automatic logoff question.

5.   Select a file transfer protocol by typing the indicated letter, such as **Z** for Zmodem (the recommended protocol).

6. If you select Zmodem, the transfer will begin automatically. If you select another protocol, you may have to initiate the transfer yourself. (In most datacomm programs, the PAGE DOWN key initiates the download.)

If you don't know the file name

1. From the Main Menu, type **F** to access the Files Menu. For a list of file areas, type **L** twice. (If you do not type the second *L*, you will list all of the files on the BBS.)

2. Mark the file areas you would like to examine by typing each file area's list number and pressing ENTER.

3. Enter **L** to list all the files in the selected file areas. Enter **C** to go forward in the file list and **P** to go back.

4. Mark one or more files for download by entering **M**, the list numbers of the files, and pressing ENTER.

5. Enter **D**. You will see a list of the files you have marked. Enter **E** if you would like to edit the list; otherwise enter **D** again to start the download process.

6. Select a file transfer protocol by typing the indicated letter, such as **Z** for Zmodem (the recommended protocol).

7. If you select Zmodem, the file will transfer automatically. If you select another protocol, you may have to initiate the transfer yourself. (In most communications programs, the PAGE DOWN key initiates the download.)

8. When the download is complete, enter **S** to return to the File Menu.

Reading a Message

When you log on, the BBS will tell you if you have a personal message (mail). At the prompt **Would you like to read it now?**, type **R** to read the message. This is the only point at which you can read your mail, since you cannot read any messages from the Message Menu.

Leaving a Message

The Multi-Tech BBS has no public discussion area. To leave a personal message, select the Message Menu by typing **M** at the Main Menu. Type **E**, then press ENTER to select the Sysop conference. Enter the name of the recipient (or "Sysop"), the subject, and the message text. Press ESC to finish,

then type **S** to save the message and exit. To abort the message at any point, leave any of the fields blank and press ENTER.

Bulletins

When you log on, the BBS will ask if you would like to view the bulletin menu. The bulletins are menu-driven; to read a bulletin, enter its number. You can also access the bulletins by typing **B** at the Main Menu.

About the Internet

Multi-Tech is a commercial provider on the Internet, and we retrieve e-mail messages from the following mailboxes on a periodic basis:

tsupport@multitech.com   Technical Support
mtsmktg@multitech.com   Marketing Dept.
mtssales@multitech.com   Sales Dept.
international@multitech.com International Marketing & Sales
writers@multitech.com   Publications Dept.

Multi-Tech's presence includes a Web site at:

http://www.multitech.com

and an ftp site at:

ftp://ftp.multitech.com

The ftp server mirrors the Multi-Tech BBS.

About CompuServe

In addition to the BBS, Multi-Tech provides support through CompuServe's Modem Vendor Forum (GO MODEMVEN) under GO MULTITECH. You can also download manuals, Help files, drivers, Microsoft Mail scripts, and product tips and descriptions from the forum's Multi-Tech library. Refer to your CompuServe documentation for special operating procedures.

About the Multi-Tech Fax-Back Service

Multi-Tech's fax-back service provides 24-hour access to sales, marketing, and technical literature for customers in the USA. Dial (612) 717-5888, follow the voice prompts, and enter the document number for either the Sales and Marketing catalog or the Technical Support catalog of documents. For convenience, write your fax number in the following space:
_____.

From the Sales and Marketing catalog, you can request to have newsletters, white papers, press releases, brochures, and other marketing literature faxed to you. From the Technical Support catalog, you can request basic modem operation information and troubleshooting guides. With either catalog, simply enter the FB Doc. number of the literature you wish to receive.

Index

A

access times, user, 43
adding an IP site, 13
Agent mode, 12
agent site, creating, 13
analyzing data, 14
Arcnet, 62
AT commands, 28

B

BBS, Multi-Tech, 71–73
blacklist, 49

C

Call Back Queue window, 54
call pool, 31
Call Traffic window, 39, 48, 53
Callback Queue window, 48
callback security, 21, 36
   description, 36
   types, 37
callback timer, 36
commands, configuration, 19
community settings, 13
CompuServe, 74
computer requirements, 6
configuration
   commands, 19
   conditions, 31
   planning, 29–32
   procedures, 32–33
configuration files, 19
   assigning to modem, 33
   creating, 19, 32
   sending to remote rack, 20
Configuration Manager, 18, 32
configuring

for UNIX system, 29
   modem groups, 33
   modems, 27–33, 58
   MultiCommManager, 8–13
   remote IP sites, 13
connection history, 53
creating
   a group, 27
   an agent site, 13
   modem configuration files, 32

D

data analysis, 14
database editor, 21
default modem settings, 28
deleting an IP site, 13
dial backup, 31
dial-up lines, 31
displaying
   objects, 11
   remote IP sites, 12
dragging objects, 26

E

editing an IP site, 13
error
   conditions, 52
   messages, 64–68
Explorer window, 9

F

Fault and Status Events window, 52
fault management, 58
   messages, 64–68
   setup, 59
faults and status events, viewing, 52
fax server, 29, 30
fax-back service, 74